Docket No.: 22040-00037-US1
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Makoto Izawa et al.

Application No.: 10/710,982 Confirmation No.: 4981

Filed: August 16, 2004 Art Unit: N/A

For: ENCRYPTION APPARATUS, ENCRYPTION METHOD, AND ENCRYPTION SYSTEM Examiner: Not Yet Assigned

CLAIM FOR PRIORITY AND SUBMISSION OF DOCUMENTS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant hereby claims priority under 35 U.S.C. 119 based on the following prior foreign application filed in the following foreign country on the date indicated:

Country	Application No.	Date
Japan	2002-134680	May 9, 2002

In support of this claim, a certified copy of the said original foreign application is filed herewith.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 22-0185, under Order No. 22040-00037-US1 from which the undersigned is authorized to draw.

Dated: August 17, 2004
23525_1

Respectfully submitted,

By Larry J. Hume
Larry J. Hume
Registration No.: 44,163
CONNOLLY BOVE LODGE & HUTZ LLP
1990 M Street, N.W., Suite 800
Washington, DC 20036-3425
(202) 331-7111
(202) 293-6229 (Fax)
Attorney for Applicant

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed th this Office.

出願年月日
Date of Application: ２００２年　５月　９日

出願番号
pplication Number: 特願２００２－１３４６８０

ST. 10/C] : [ＪＰ２００２－１３４６８０]

願人
plicant(s): 新潟精密株式会社
株式会社マイクロ総合研究所

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００４年　７月　５日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

【書類名】　特許願
【整理番号】　14NS1428
【提出日】　平成14年 5月 9日
【あて先】　特許庁長官殿
【国際特許分類】　G09C　1/00
【発明者】
　【住所又は居所】　東京都品川区南品川２丁目２番５号　株式会社マイクロ総合研究所内
　【氏名】　井澤　誠
【発明者】
　【住所又は居所】　東京都品川区南品川２丁目２番５号　株式会社マイクロ総合研究所内
　【氏名】　成田　宏光
【発明者】
　【住所又は居所】　埼玉県上尾市緑丘４丁目７番１７号
　【氏名】　岡本　明
【特許出願人】
　【識別番号】　591220850
　【氏名又は名称】　新潟精密株式会社
【特許出願人】
　【住所又は居所】　東京都品川区南品川２丁目２番５号
　【氏名又は名称】　株式会社マイクロ総合研究所
【代理人】
　【識別番号】　100105784
　【弁理士】
　【氏名又は名称】　橘　和之
　【電話番号】　049-249-5122

【手数料の表示】

【予納台帳番号】　070162

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0006161

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号装置および方法、暗号システム

【特許請求の範囲】

【請求項１】　複数のポートを有し、少なくとも１つのポートに暗号処理機能を有する端末が直接または間接的に接続される暗号装置であって、

上記暗号処理機能を有する端末との間で暗号化によるセキュリティを終端するためにデータの暗号化処理および復号化処理を行う暗号／復号手段と、

上記複数のポートのうち一のポートより入力され上記暗号／復号手段により暗号化処理または復号化処理が施されたデータを、ルーティング処理をすることなく他のポートにそのまま出力するブリッジ手段とを備えたことを特徴とする暗号装置。

【請求項２】　上記暗号／復号手段は、上記暗号処理機能が導入された端末との間では暗号化されたデータの通信を行うとともに、上記暗号処理機能が導入されていない端末との間では暗号化されていないデータの通信を行うために上記暗号化処理および上記復号化処理を行うことを特徴とする請求項１に記載の暗号装置。

【請求項３】　複数のポートを有し、少なくとも１つのポートに暗号処理機能を有する端末が直接または間接的に接続される暗号装置であって、

上記複数のポートのうち一のポートより入力され物理層およびデータリンク層を介して渡されたデータに対して暗号化処理または復号化処理を行う暗号／復号手段と、

上記暗号／復号手段により暗号化処理または復号化処理が施されたデータを、ネットワーク間のルーティング制御を行うネットワーク層に渡すことなくデータリンク層および物理層を介して他のポートより出力するようにするブリッジ手段とを備えたことを特徴とする暗号装置。

【請求項４】　上記暗号化処理および上記復号化処理の制御に関する設定情報を記憶する設定情報記憶手段を備え、

上記暗号／復号手段は、上記設定情報記憶手段に記憶されている設定情報と、上記一のポートより入力されたパケットに付加されているヘッダ情報とを照合し

て上記暗号化処理および上記復号化処理の制御を行うことを特徴とする請求項３に記載の暗号装置。

【請求項５】　複数のポートを有し、少なくとも１つのポートに暗号処理機能を有する端末が直接または間接的に接続される暗号装置において暗号化処理または復号化処理を行う方法であって、

上記複数のポートのうち一のポートより入力され物理層およびデータリンク層を介して渡されたデータに対して暗号化処理または復号化処理を行い、これにより得られたデータを、ネットワーク間のルーティング制御を行うネットワーク層に渡すことなくデータリンク層および物理層を介して他のポートより出力するようにしたことを特徴とする暗号方法。

【請求項６】　暗号処理機能が導入された端末と、請求項１に記載の暗号装置とが無線または有線のネットワークを介して接続されて成ることを特徴とする暗号システム。

【請求項７】　暗号処理機能が導入された端末と、暗号処理機能が導入されていない端末との間に、請求項２に記載の暗号装置が無線または有線のネットワークを介して接続されて成ることを特徴とする暗号システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は暗号装置および方法、暗号システムに関し、特に、ネットワーク上で外部から攻撃されることによる情報の盗聴や改ざん等のリスクを低減するために情報の暗号化／復号化を行う装置および方法、これを適用したシステムに用いて好適なものである。

【０００２】

【従来の技術】

パーソナルコンピュータ（パソコン）をスタンドアロンで用いる場合は、パソコン内部の情報が盗み出されたり、改ざんされたり、破壊されたりする危険性は少ない。しかし、パソコンをインターネット等のネットワークに接続すると、やり取りされる情報は多くのネットワークをルーティングされていくことから、そ

の途中において盗聴や改ざん等の行われる危険性が一気に増大する。

【０００３】

この問題を解決するための仕組みの１つとして、情報の暗号化がある。すなわち、送信側のパソコンで情報を暗号化して相手に送り、受信側のパソコンでこれを復号化して利用する。このようにすれば、ネットワークの途中で情報が盗聴されたとしても、情報が暗号化されているために、情報自体が見られる可能性が少なくなる。また、改ざんのリスクも低減される。

【０００４】

【発明が解決しようとする課題】

しかしながら、暗号を利用するためには、暗号通信しようとする端末の全てに専用の暗号ソフトをインストールし、様々な設定をしなければならない。ところが、各種端末が接続されるネットワークは、インターネットの他に、企業内のＬＡＮ（Local Area Network）なども存在する。そのＬＡＮ内には、プリンタやファクシミリなど物理的に暗号ソフトをインストールできない端末や、プリントサーバやデータベースサーバなど動作安定上等の問題から余分なソフトをインストールすることが好ましくない端末、ＯＳ（オペレーティングシステム）がなく単なるネットワークターミナルとして機能する端末なども存在する。そのため、一般的に企業内ＬＡＮの中では、暗号を利用することは難しかった。

【０００５】

ところが、ＬＡＮの多くはインターネットに接続されており、必要に応じてＬＡＮ内のパソコンからインターネットにアクセスして情報のやり取りを行うことができるようになっている。しかし、このようにＬＡＮがインターネットに接続されていると、外部からの不正侵入や攻撃によって、ＬＡＮ内部の機密情報が盗まれたり改ざんされたりする危険性が出てくる。

【０００６】

そこで、アクセス権を持たない第三者がＬＡＮ内に不正に侵入するのを防ぐために、ファイアウォールが利用される。ファイアウォールは、一般的には１台のサーバをＬＡＮとインターネットとの接続部に用い、ここで専用のソフトウェアを動作させることによって機能する。しかし、ファイアウォールを設置しても、

ネットワーク上に存在するセキュリティホールを攻撃することによって不正侵入が行われることが少なくない。一旦不正侵入が行われると、内部の情報は暗号化されていないため、盗聴や改ざんが容易にできてしまうという問題があった。

【０００７】

なお、従来、インターネット上に流れるデータをルーティングする中継機であるルータに暗号機能を持たせたものが存在する。例えばＶＰＮ（Virtual Private Network）ルータがそれである。このＶＰＮルータを用いれば、端末に専用の暗号ソフトをインストールしなくても、ＶＰＮルータ間で暗号通信を行うことが可能となる。

【０００８】

しかしながら、このＶＰＮルータは、インターネットを利用して複数のＬＡＮを接続するために設けられる仮想専用線上の中継機として用いられるものである。そのため、ＬＡＮどうしがやり取りする情報を途中のインターネット上において暗号化することはできるが、ＬＡＮ内において情報を暗号化することはできないという問題があった。

【０００９】

また、ＶＰＮルータにおいて暗号化を行うためには、ルータが必ず通信用のＩＰアドレスを持つことが必要となる。以下に、このことについて図８を用いて説明する。図８は、従来のＶＰＮルータおよびこれに接続されるパソコンにおけるプロトコルの階層構造を示す図である。

【００１０】

図８に示すように、通信しようとする２台のパソコン１０１，１０２はそれぞれ１つのポート１０５，１０６を有し、その中継機となるＶＰＮルータ１０３，１０４はそれぞれ２つのポート（１０７，１０８），（１０９，１１０）を有している。ＶＰＮルータ１０３の各ポート１０７，１０８に対して物理層、ＭＡＣ層（データリンク層）、ＩＰ－Ｓｅｃが個別に設けられ、各ポート１０７，１０８に共通なものとしてＩＰ層（ネットワーク層）、ＴＣＰ／ＵＤＰ層（トランスポート層）が設けられている。ＶＰＮルータ１０４の各ポート１０９，１１０についても同様である。

【００１１】

層が深くなるほどユーザからは遠くなり、逆に層が浅くなるほどユーザに近くなる。各パソコン１０１，１０２のＩＰ層よりも上位層には、ＴＣＰ／ＵＤＰ層およびアプリケーション層（共に図示せず）が存在し、ユーザが使用するアプリケーションと下の層との橋渡しが行われる。

【００１２】

データの送信側では、上位層から下位層に向かって各層を通過するごとにデータが変換されるとともに、それぞれの層間でデータ伝送を可能にするためのヘッダが付加されていく。逆に、データの受信側では、各層宛てのヘッダを参照して各層で必要なデータが抽出される。そして、抽出されたデータは上位層へ引き渡され、最終的にアプリケーション層を介してユーザに届けられる。

【００１３】

以下に、それぞれの層の機能について説明する。ＴＣＰ／ＵＤＰ層は、データを渡すべきアプリケーションの特定や、パケットの状態の管理などを行うレイヤである。データ送信側においては、上位層（アプリケーション層）から渡されたデータを相手のどのアプリケーションに渡すべきかを認識し、宛先ポート番号をデータに付加して下位層（ネットワーク層）に渡す。一方、データ受信側においては、下位層から渡されたパケットについて、通信の状態等によって抜けが生じていないかどうかを監視する。

【００１４】

ＩＰ層は、複数のネットワークにまたがった端末間のデータ転送あるいはデータ中継に関する取り決めや制御を行うためのレイヤである。通信相手となる送信側と受信側のパソコン１０１，１０２にはそれぞれ異なるＩＰアドレス①，⑥が割り振られており、これらを明確にすることによって、end to endによる論理的な通信経路が決定する。２つのポート（１０７，１０８），（１０９，１１０）を有するＶＰＮルータ１０３，１０４の場合、ＩＰアドレスはポート毎に別個に割り振られる。

【００１５】

ＭＡＣ（Media Access Control）層は、隣接機器のノード間で信頼性の高いデ

ータ伝送を保証するためのレイヤであり、製造段階で各機器に割り当てられた物理的なＭＡＣアドレスを有する。データ送信側においては、ＩＰ層で通信相手のＩＰアドレスが明確になると、その下位に位置するＭＡＣ層において、確立された相手のＩＰアドレスをもとに、経由する次の機器（物理的に接続されている隣接ノード）の宛先を決定する。一方、データ受信側においては、ＭＡＣアドレスをもとに自分宛のパケットであることを認識した後、その上位層のＩＰ層でＩＰアドレスを解析し、そのパケットを他の機器に対して更にルーティングするか自分に取り込むかを判断する。

【００１６】

物理層は、上位層から渡されたデータを電気信号や光信号に変換し、同軸ケーブルや光ファイバケーブル等の伝送媒体１１１を介して実際のデータ伝送を行ったり、伝送媒体１１１から送られてきた電気信号や光信号を上位層で認識可能なデータに変換し、それを上位層に渡したりするためのレイヤである。物理層の上位層であるＭＡＣ層では、物理層の通信インタフェースに依存した手法に従って上述の処理を行う。

【００１７】

ＩＰ－Ｓｅｃは、データの暗号化処理および復号化処理を行う機能部である。すなわち、ＭＡＣ層からＩＰ層に渡されるデータを取得して、当該データの暗号化処理および暗号の復号化処理を行う。

【００１８】

このような階層構造を有するＶＰＮルータ１０３，１０４を用いてパソコン１０１，１０２間で暗号通信を行う場合、ＶＰＮルータ１０３では、例えば一方のパソコン１０１から他方のパソコン１０２宛てに送られてきたＩＰパケットを第１のポート１０７で受信し、ＩＰ層までパケットを順次引き渡して分解する。このとき、パケット中から抽出したデータをＩＰ－Ｓｅｃで暗号化する。そして、パケットヘッダ中に含まれている宛先ＩＰアドレスをもとに、ルータ自身が持つルーティングテーブルを参照して次の転送ノードを決定し、ＩＰ層から物理層へと再度パケットを組み立てて第２のポート１０８から送出する。

【００１９】

ＶＰＮルータ１０３の第２のポート１０８から出力された暗号化パケットは、ＶＰＮルータ１０４の第１のポート１０９で受信される。ＶＰＮルータ１０４は、受信した暗号化パケットをＩＰ層まで順次引き渡して分解し、パケット中から抽出したデータをＩＰ－Ｓｅｃで復号化する。そして、パケットヘッダ中に含まれている宛先ＩＰアドレスをもとに、ルータ自身が持つルーティングテーブルを参照して次の転送ノードを決定し、ＩＰ層から物理層へと再度パケットを組み立てて第２のポート１１０から送出する。

【００２０】

この第２のポート１１０から出力されたＩＰパケットは、パソコン１０２で受信される。この受信されたＩＰパケットは物理層、ＭＡＣ層、ＩＰ層を介して上位層へと順次引き渡されて分解され、最終的に図示しないアプリケーション層を介してユーザにデータが届けられる。以上の手順により、パソコン１０１，１０２が暗号ソフトを備えていなくても、ＶＰＮルータ１０３，１０４間で暗号通信をすることが可能となる。

【００２１】

図８に示したシステムの場合、ＶＰＮルータ１０３，１０４の両側に異なるネットワーク（パソコン１０１を有するネットワークＡとパソコン１０２を有するネットワークＢ）が存在し、これが集まってインターネットを構成している。そのため、それぞれのネットワーク毎に異なるネットワークアドレスが割り振られる。よって、これらの異なるネットワーク間をルーティング（経路選択、場合によってパケットの破棄、パケットの分割あるいは統合等）するＶＰＮルータ１０３，１０４も、異なるＩＰアドレスを持つことが必須であり、そのために煩雑なアドレス設定作業を行わなければならないという問題があった。

【００２２】

また、ＶＰＮルータ１０３，１０４では第１のポート１０７，１０９に接続されるネットワークと第２のポート１０８，１１０に接続されるネットワークは一般的に異なるものであり、そのためにポート毎に異なるＩＰアドレスを設定する必要がある。よって、ＶＰＮルータ１０３，１０４の入力と出力とでＩＰアドレスが変わってしまう。そのため、ネットワーク上にある端末間にＶＰＮルータを

挿入したり、あるいは端末間からＶＰＮルータを外したりする際には、ＶＰＮルータ自身のアドレス設定を行うだけでなく、当該ＶＰＮルータに接続される端末のアドレス設定も変更する必要があり、各種の煩雑な作業を行わなければならないという問題があった。

【００２３】

例えば、図８の例においてＶＰＮルータ１０３，１０４を接続しない状態で通信を行う場合は、パソコン１０１，１０２は同一のネットワーク内に存在することになるので、ネットワークアドレスが共に同じとなり、パソコン１０１，１０２間で直接の通信が可能である。この場合、パソコン１０１からパソコン１０２に送信するパケットのＩＰアドレスは、図９（ａ）のようになる。すなわち、送信側であるパソコン１０１の送信元ＩＰアドレス①と、受信側であるパソコン１０２の宛先ＩＰアドレス⑥のネットワークアドレスには、同じネットワークアドレスＡを設定すれば良い。

【００２４】

これに対し、パソコン１０１とパソコン１０２との間にＶＰＮルータ１０３，１０４を挿入した場合は、送信されるパケットのＩＰアドレスは図９（ｂ）のようになる。すなわち、パソコン１０１，１０２は異なるネットワークに存在することになるので、送信元ＩＰアドレス①と宛先ＩＰアドレス⑥には、異なるネットワークアドレスＡ，Ｂを設定しなければならない。

【００２５】

このように、パソコン１０１とパソコン１０２との間にＶＰＮルータ１０３，１０４を挿入したり、あるいはその逆にＶＰＮルータ１０３，１０４を取り外したりすると、パソコン１０１，１０２の属するネットワークが変わる。したがって、それに合わせて、パソコン１０１，１０２のデフォルトゲートウェイのアドレス（自分と異なるネットワークに対して通信をする場合の宛先ＩＰアドレス（ＶＰＮルータ１０３，１０４のポート１０７，１１０））や、パソコン１０１，１０２の何れかのＩＰアドレスの設定を変更する必要が生じる。

【００２６】

以上のように、従来のＶＰＮルータでは、その接続の有無によって透過性を保

つことが困難であり、システムの導入時やメンテナンス時には多大な作業をしなければならないという問題があった。

【００２７】

本発明は、このような問題を解決するために成されたものであり、専用の暗号ソフトをインストールできない端末を有する企業内ＬＡＮの中でも暗号を利用して、外部からの不正侵入や攻撃によってＬＡＮ内部の機密情報が盗まれたり改ざんされたりする危険性を低減できるようにすることを目的とする。

また、本発明は、アドレス設定などの煩雑な作業を行うことなく、企業内ＬＡＮで暗号を利用できるようにすることを目的とする。

【００２８】

【課題を解決するための手段】

本発明の暗号装置は、複数のポートを有し、少なくとも１つのポートに暗号処理機能を有する端末が直接または間接的に接続される暗号装置であって、上記暗号処理機能を有する端末との間で暗号化によるセキュリティを終端するためにデータの暗号化処理および復号化処理を行う暗号／復号手段と、上記複数のポートのうち一のポートより入力され上記暗号／復号手段により暗号化処理または復号化処理が施されたデータを、ルーティング処理をすることなく他のポートにそのまま出力するブリッジ手段とを備えたことを特徴とする。

【００２９】

本発明の他の態様では、上記暗号／復号手段は、上記暗号処理機能が導入された端末との間では暗号化されたデータの通信を行うとともに、上記暗号処理機能が導入されていない端末との間では暗号化されていないデータの通信を行うために上記暗号化処理および上記復号化処理を行うことを特徴とする。

【００３０】

本発明のその他の態様では、複数のポートを有し、少なくとも１つのポートに暗号処理機能を有する端末が直接または間接的に接続される暗号装置であって、上記複数のポートのうち一のポートより入力され物理層およびデータリンク層を介して渡されたデータに対して暗号化処理または復号化処理を行う暗号／復号手段と、上記暗号／復号手段により暗号化処理または復号化処理が施されたデータ

を、ネットワーク間のルーティング制御を行うネットワーク層に渡すことなくデータリンク層および物理層を介して他のポートより出力するようにするブリッジ手段とを備えたことを特徴とする。

【００３１】

本発明の更に別の態様では、上記暗号化処理および上記復号化処理の制御に関する設定情報を記憶する設定情報記憶手段を備え、上記暗号／復号手段は、上記設定情報記憶手段に記憶されている設定情報と、上記一のポートより入力されたパケットに付加されているヘッダ情報とを照合して上記暗号化処理および上記復号化処理の制御を行うことを特徴とする。

【００３２】

また、本発明の暗号方法は、複数のポートを有し、少なくとも１つのポートに暗号処理機能を有する端末が直接または間接的に接続される暗号装置において暗号化処理または復号化処理を行う方法であって、上記複数のポートのうち一のポートより入力され物理層およびデータリンク層を介して渡されたデータに対して暗号化処理または復号化処理を行い、これにより得られたデータを、ネットワーク間のルーティング制御を行うネットワーク層に渡すことなくデータリンク層および物理層を介して他のポートより出力するようにしたことを特徴とする。

【００３３】

また、本発明の暗号システムは、暗号処理機能が導入された端末と、請求項１に記載の暗号装置とが無線または有線のネットワークを介して接続されて成ることを特徴とする。

【００３４】

本発明の他の態様では、暗号処理機能が導入された端末と、暗号処理機能が導入されていない端末との間に、請求項２に記載の暗号装置が無線または有線のネットワークを介して接続されて成ることを特徴とする。

【００３５】

【発明の実施の形態】

以下、本発明の一実施形態を図面に基づいて説明する。

図１は、本実施形態の暗号装置を適用した暗号システムの全体構成例を示す図

である。

【００３６】

図１において、１は本実施形態の暗号装置であり、２つのポートを有し、一方のポートにはネットワークプリンタ２、ＤＢサーバ３、ネットワークターミナル４などのデバイスが接続され、他方のポートにはハブ５が接続されている。この暗号装置１は、ネットワークプリンタ２、ＤＢサーバ３、ネットワークターミナル４などのデバイスと、ハブ５との間でデータの中継を行う。

【００３７】

ネットワークプリンタ２は、暗号ソフトを物理的にインストールできない端末である。ＤＢサーバ３は、動作安定上等の問題から余分な暗号ソフトをインストールすることが好ましくない端末である。ネットワークターミナル４は、ＯＳがなく暗号ソフトを動作させることができない端末である。したがって、これらの端末２～４には暗号ソフトはインストールされていないものとする。

【００３８】

また、ハブ５は、物理層においてデータを中継する機器であり、上述した暗号装置１の他に、無線通信用のアクセスポイント６とデスクトップパソコン７とが接続されている。すなわち、この場合のハブ５は、暗号装置１と、アクセスポイント６およびデスクトップパソコン７との間でデータの中継を行う。

【００３９】

さらに、上記アクセスポイント６には、デスクトップパソコン８とラップトップパソコン９とが無線により接続されている。デスクトップパソコン７，８およびラップトップパソコン９には、データの暗号化および復号化を行うための暗号ソフトがインストール可能であり、実際にインストールされているものとする。

【００４０】

このような構成により、暗号ソフトがインストールされていないネットワークプリンタ２、ＤＢサーバ３およびネットワークターミナル４と、暗号ソフトがインストールされているパソコン７～９との間で、暗号装置１、ハブ５およびアクセスポイント６を介してデータ通信が行われる。

【００４１】

その際、暗号装置１は、暗号ソフトがインストールされているパソコン７～９との間では暗号化されたデータの通信を行うとともに、暗号ソフトがインストールされていない端末２～４との間では暗号化されていないデータの通信を行うために暗号化処理および暗号の復号化処理を行う。

【００４２】

例えば、デスクトップパソコン７からネットワークプリンタ２にデータを送出してプリントアウトするときは、まずデスクトップパソコン７にインストールされている暗号ソフトを用いてデータを暗号化し、ハブ５を介して暗号装置１に供給する。次に暗号装置１は、受け取ったデータを復号化し、ネットワークプリンタ２に送出する。

【００４３】

また、例えばＤＢサーバ３にて管理されているデータをラップトップパソコン９に取り込むときは、ＤＢサーバ３は、与えられる要求に応じて該当するデータを暗号装置１に供給する。この暗号化されていないデータを受け取った暗号装置１は、そのデータを暗号化し、ハブ５およびアクセスポイント６を介してラップトップパソコン９に送信する。ラップトップパソコン９は、受け取ったデータを復号化し、所望の処理に利用する。

【００４４】

以上の説明から明らかなように、本実施形態の暗号装置１を用いることによって、専用の暗号ソフトをインストールできない端末２～４を有する企業内ＬＡＮの中でも、暗号を利用することが可能となる。これにより、外部からの不正侵入や攻撃によってＬＡＮ内部の機密情報が盗まれたり改ざんされたりする危険性が少ないセキュアなネットワーク１０を構築することができる。

【００４５】

なお、暗号装置１と各端末２～４との間において暗号は利用できないが、これらを繋ぐケーブル１１は物理的に短い配線であり、この部分が外部アタックされることによって盗聴や改ざんが行われる可能性は極めて低いので、セキュリティ上で特に問題となることはない。

【００４６】

図２は、本実施形態の暗号装置を適用した暗号システムの他の構成例を示す図である。なお、この図２において、図１に示した構成要素と同一の機能を有する構成要素には同一の符号を付している。図２に示すように、本実施形態の暗号装置１は、一方のポートにインターネット２０が接続され、他方のポートにハブ５が接続されている。インターネット２０の先には、図１に示したネットワークプリンタ２、ＤＢサーバ３、ネットワークターミナル４などのように暗号ソフトをインストールできない端末、あるいは、パソコン７～９のように暗号ソフトがインストールされた端末が複数台接続されている。

【００４７】

図１に示した例では、１台の暗号装置１に対して１台のデバイスが接続されており、１台のデバイスに関する暗号／復号処理を１台の暗号装置１が専用で行っていた。すなわち、図１に示す暗号装置１は、暗号ソフトがインストールされたパソコン７～９と、暗号ソフトがインストールされていない１台のデバイスとの間に接続され、暗号ソフトがインストールされたパソコン７～９との間で暗号化によるセキュリティを終端していた。

【００４８】

これに対して、図２に示す例では、暗号装置１は、暗号ソフトがインストールされたパソコン７～９と、インターネット２０に接続された複数台のデバイスとの間に接続されている。このように、本実施形態の暗号装置１は、複数台のデバイスに対して暗号化によるセキュリティを終端することも可能である。この場合、暗号装置１は、接続されているデバイスの数だけデータパスを有し、それぞれのデバイス毎に異なる暗号鍵で暗号／復号処理を行う。

【００４９】

上記複数台のデバイスは、暗号ソフトがインストールされていても良いし、インストールされていなくても良い。暗号ソフトがインストールされている場合には、セキュアネットワーク１０の外部にあるインターネット２０上でも暗号を利用することができる。なお、上記複数台のデバイスは、インターネット２０を介して接続されている必要は必ずしもなく、暗号装置１に直接接続しても良い。この場合、暗号装置１は２つ以上のポートを有することになる。

【００５０】

図３は、本実施形態の暗号装置を適用した暗号システムの更に別の構成例を示す図である。なお、この図３において、図１に示した構成要素と同一の機能を有する構成要素には同一の符号を付している。図３に示す例も図２の例と同様に、１台の暗号装置１が複数台のデバイスに対して暗号化によるセキュリティを終端する例である。

【００５１】

図３に示す例では、セキュアネットワーク１０の内部は、３台のパソコン７～９が全てアクセスポイント６に無線ＬＡＮにて接続されている。アクセスポイント６は、暗号装置１を介してインターネット２０に接続されている。

【００５２】

図４は、図１に示した暗号システムにおいて、暗号装置１およびこれに直接および間接的に接続されるＤＢサーバ３およびラップトップパソコン９におけるプロトコルの階層構造を示す図である。図４に示す例では、ＤＢサーバ３には暗号ソフトがインストールされておらず（ＩＰ－Ｓｅｃがない）、ラップトップパソコン９には暗号ソフトがインストールされている（ＩＰ－Ｓｅｃを有する）。このＤＢサーバ３およびラップトップパソコン９の間に、本実施形態の暗号装置１が接続されている。ここでは、ＤＢサーバ３にて保存されているデータを暗号装置１に送り、ここでデータを暗号化してパソコン９に送るような利用形態を想定している。

【００５３】

図４に示すように、ＤＢサーバ３およびパソコン９はそれぞれ１つのポート３１，３２を有し、その中継機となる暗号装置１は２つのポート３３，３４を有している。暗号装置１の各ポート３３，３４に対して物理層およびＭＡＣ層（データリンク層）が個別に設けられ、各ポート３３，３４に共通なものとしてＩＰ－Ｓｅｃ（暗号／復号処理機能）、ＩＰ層（ネットワーク層）およびＴＣＰ／ＵＤＰ層（トランスポート層）が設けられている。このように、本実施形態の暗号装置１は、ＩＰ－Ｓｅｃにより２つのポート３３，３４間をブリッジさせているところに特徴がある。

【００５４】

本実施形態の暗号装置１では、ＤＢサーバ３とパソコン９との間におけるデータ転送に関してはＩＰ層およびＴＣＰ／ＵＤＰ層は用いず、ＩＰ層よりも下位層で処理を行う。すなわち、第１のポート３３より入力されたデータに対してＩＰ－Ｓｅｃで暗号化処理を行い、それにより得られたデータを、ＩＰ層にてルーティングすることなく（ＩＰ層に渡すことなく）他方のポートにそのまま渡して出力する。

【００５５】

すなわち、ＤＢサーバ３にて作成されたパケットデータは、当該ＤＢサーバ３のＭＡＣ層、物理層を通って送信され、暗号装置１の第１のポート３３より受信される。受信されたパケットデータは物理層、ＭＡＣ層を通ってＩＰ－Ｓｅｃに渡され、ここで暗号化処理が行われる。この暗号化されたパケットデータは、ＭＡＣ層および物理層を通って第２のポート３４より送信される。

【００５６】

第２のポート３４より送信されたパケットデータは、パソコン９で受信され、物理層、ＭＡＣ層を通ってＩＰ－Ｓｅｃに渡されて、暗号が復号化される。そして、復号化されたデータがＩＰ層を通って図示しないアプリケーション層に渡される。これにより、ＤＢサーバ３が暗号ソフトを備えていなくても、パソコン９に対して暗号化されたデータを送信することが可能となる。

【００５７】

なお、本実施形態においてＩＰ層およびＴＣＰ／ＵＤＰ層は、暗号装置１自身に暗号化／復号化に関する各種の情報を設定する際に利用される。例えば、ある端末とある端末との間では暗号通信を行うが、他の端末との間では暗号通信を行わないなどといった暗号／復号処理の有無、ある端末とある端末との間ではパケットを破棄するなどといった通信の可否、暗号通信を行う場合における暗号化のレベル、暗号化を行う時間帯、暗号鍵などに関する種々の情報を暗号装置１に設定する場合には、ＩＰ層およびＴＣＰ／ＵＤＰ層を使用する。

【００５８】

この種の設定情報は、ＩＰ－Ｓｅｃブリッジの機能によってメモリ上に保持さ

れる。ＩＰ－Ｓｅｃは、当該メモリに保持されている設定情報と、ポート３３，３４より入力されたパケットに付加されているヘッダ情報（例えば、送信元ＩＰアドレスおよび宛先ＩＰアドレス）とを照合して、暗号／復号処理の制御などを行う。

【００５９】

このように、本実施形態の暗号装置１では、一のポートから入力されたデータをＩＰ－Ｓｅｃで暗号化／復号化し、これにより得られたデータをＩＰ層に渡すことなく、ルーティング処理をせずにそのまま他のポートに転送するようにしているので、データ通信時に暗号装置１のＩＰアドレスを不要とすることができる。すなわち、ＩＰアドレスを持たずにＩＰ層の暗号／復号処理を行うことが可能である。そのため、暗号装置１自身に対する煩雑なＩＰアドレス設定の必要をなくすことができる。

【００６０】

また、暗号装置１の両側に接続される端末は同じネットワークに属することになり、暗号装置１の入力ポートと出力ポートとでＩＰアドレスが変わることがなくなる。これにより、暗号装置１のネットワーク上における接続の有無に関わりなく、ＩＰアドレスの透過性を保つことができる。すなわち、ネットワーク上に暗号装置１を接続したり、ネットワーク上から暗号装置１を外したりする際に、当該暗号装置１に接続される端末のアドレス設定も変更する必要がない。

【００６１】

例えば、図４のようにＤＢサーバ３とパソコン９との間に暗号装置１を挿入した場合も、暗号装置１を挿入せずにＤＢサーバ３とパソコン９との間で直接通信を行う場合も、ＤＢサーバ３とパソコン９との間を流れるパケットのＩＰアドレスは、図５に示す通りのままで不変である。したがって、暗号装置１の接続の有無によってアドレス設定を何ら変更する必要がない。

【００６２】

これにより、ネットワークシステムの導入時やメンテナンス時には、本実施形態の暗号装置１を適当な箇所にただ挿入したり、あるいはただ取り外したりするだけ良くなり、煩雑なアドレス設定は行う必要がないので、作業負荷を大幅に削

減することができる。

【００６３】

さらに、本実施形態の場合、ＭＡＣアドレスについても透過性を保つことができる。図６は、ＤＢサーバ３からパソコン９にデータを送り、その間の暗号装置１でデータを暗号化する場合におけるパケットを示す図である。また、図７は、本実施形態との比較のために、図８に示す従来のシステムにおいて一方のパソコン１０１から他方のパソコン１０２にデータを送り、その間のＶＰＮルータ１０３でデータを暗号化する場合におけるパケットを示す図である。

【００６４】

図６（ａ）および図７（ａ）は第１のポート３３，１０７にて受信するパケットを示し、図６（ｂ）および図７（ｂ）は第２のポート３４，１０８より送信するパケットを示す。なお、ＩＰ－Ｓｅｃには、データ部のみを暗号化するトランスポートモードと、パケット全てを暗号化して更に新しいヘッダを追加するトンネルモードとがある。送信パケットに関しては、これら２つのモードについてそれぞれ示している。

【００６５】

図６から明らかなように、本実施形態によれば、ＩＰアドレスだけでなく、ＭＡＣアドレスについても第１のポート３３と第２のポート３４とで異なることがなく、ＭＡＣアドレスの透過性を保つことができる。すなわち、本実施形態の暗号装置１は、ＩＰ－Ｓｅｃを有してデータの暗号／復号処理を行うことを除けば、一方のポートから入力されたデータを他方のポートにただ流すだけなので、データ通信時にはＭＡＣアドレスも不要とすることができる。

【００６６】

なお、以上に説明した実施形態は、本発明を実施するにあたっての具体化の一例を示したものに過ぎず、これによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその精神、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。

【００６７】

【発明の効果】

本発明は上述したように、暗号処理機能が導入された端末との間で暗号化によるセキュリティを終端するために暗号化処理および暗号の復号化処理を行う暗号／復号手段を備えて暗号装置を構成し、この暗号装置をネットワークを介して端末に接続するようにしたので、専用の暗号ソフトをインストールできない端末を有する企業内ＬＡＮの中でも暗号を利用することができるようになり、外部からの不正侵入や攻撃によってＬＡＮ内部の機密情報が盗まれたり改ざんされたりする危険性を低減することができる。

【００６８】

また、本発明では、暗号化処理または復号化処理が施されたデータを、ネットワーク間のルーティング制御を行うネットワーク層に渡すことなく出力するようにしたので、データ通信時に暗号装置のＩＰアドレスを不要とすることができる。また、暗号装置の入力ポートと出力ポートとでＩＰアドレスが変わることがなくなるので、暗号装置のネットワーク上における接続の有無に関わりなく、ＩＰアドレスの透過性を保つことができ、暗号装置に接続される端末のアドレス設定に関しても変更の必要をなくすことができる。これにより、アドレス設定などの煩雑な作業を行うことなく、企業内ＬＡＮで暗号を利用することができるようになる。

【図面の簡単な説明】

【図１】

本実施形態の暗号装置を適用した暗号システムの構成例を示す図である。

【図２】

本実施形態の暗号装置を適用した暗号システムの他の構成例を示す図である。

【図３】

本実施形態の暗号装置を適用した暗号システムの更に別の構成例を示す図である。

【図４】

本実施形態による暗号装置およびこれに接続されるＤＢサーバおよびパソコンにおけるプロトコルの階層構造を示す図である。

【図５】

本実施形態においてネットワーク上を流れるパケットのＩＰアドレスについて説明するための図である。

【図６】

本実施形態の暗号装置を流れるパケットのＭＡＣアドレスについて説明するための図である。

【図７】

従来のＶＰＮルータを流れるパケットのＭＡＣアドレスについて説明するための図である。

【図８】

従来のＶＰＮルータおよびこれに接続されるパソコンにおけるプロトコルの階層構造を示す図である。

【図９】

従来システムにおいてネットワーク上を流れるパケットのＩＰアドレスについて説明するための図である。

【符号の説明】

１　暗号装置

２　ネットワークプリンタ

３　ＤＢサーバ

４　ネットワークターミナル

５　ハブ

６　アクセスポイント

７，８　デスクトップパソコン

９　ラップトップパソコン

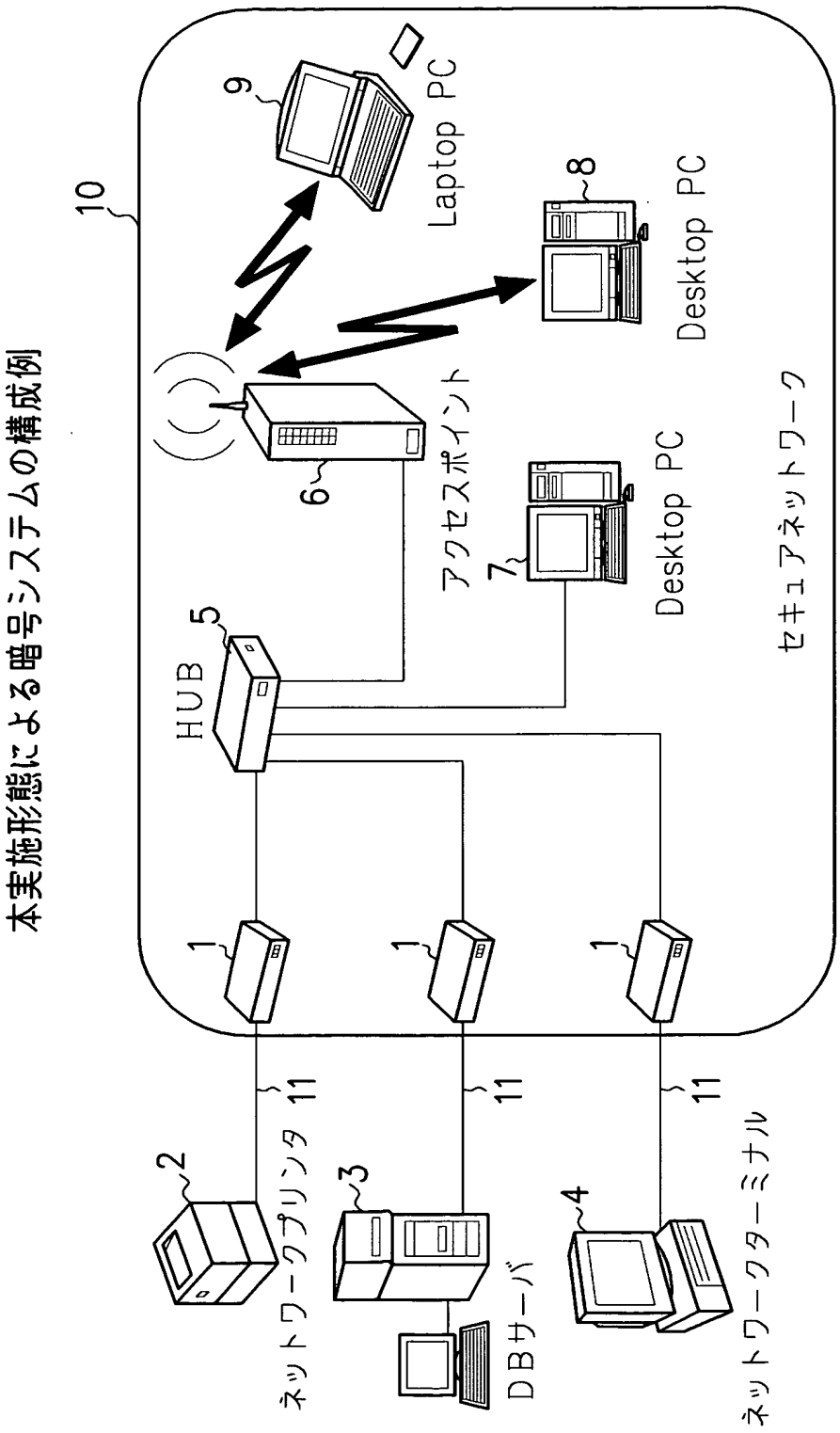
１０　セキュアネットワーク

１１　ケーブル

２０　インターネット

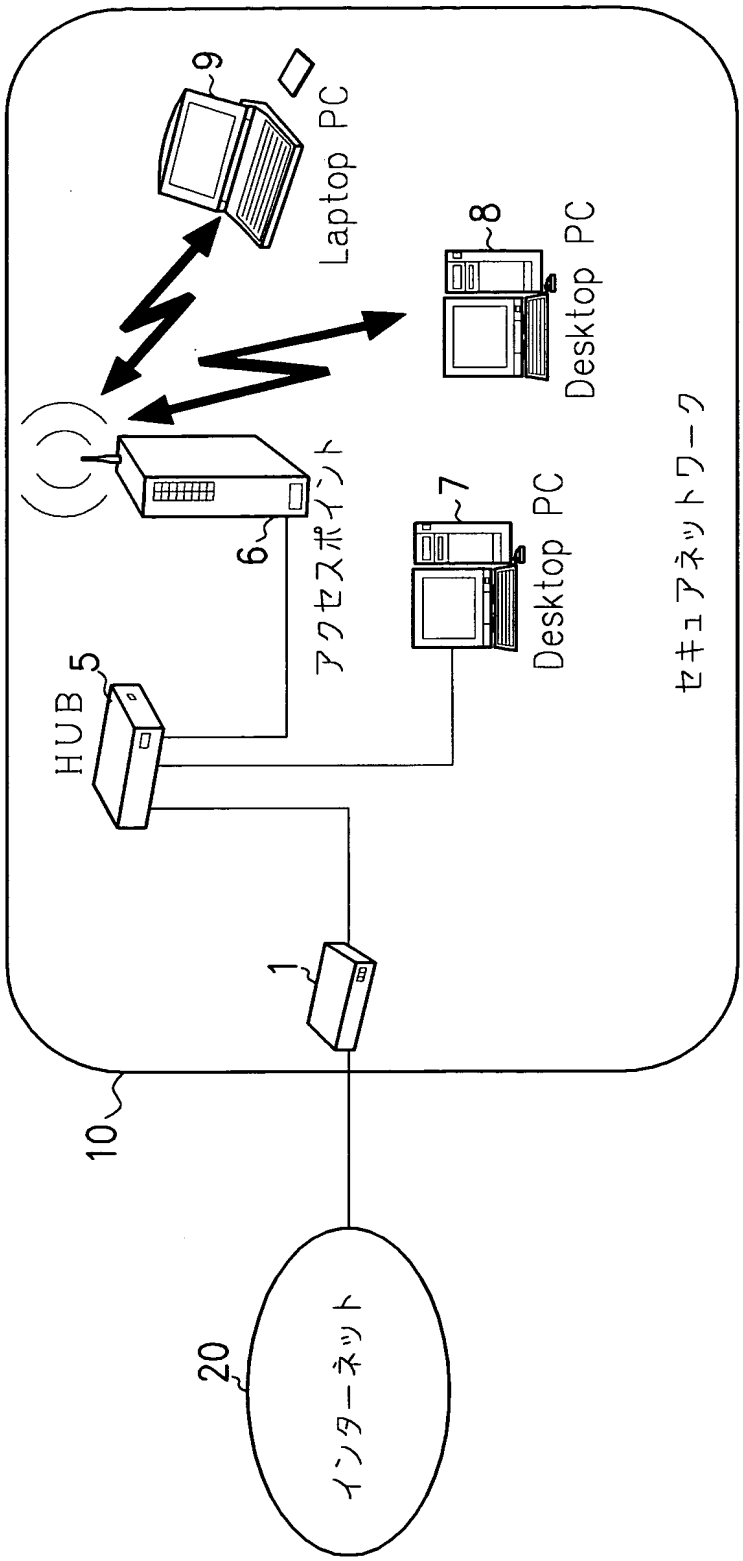
【書類名】　図面

【図１】

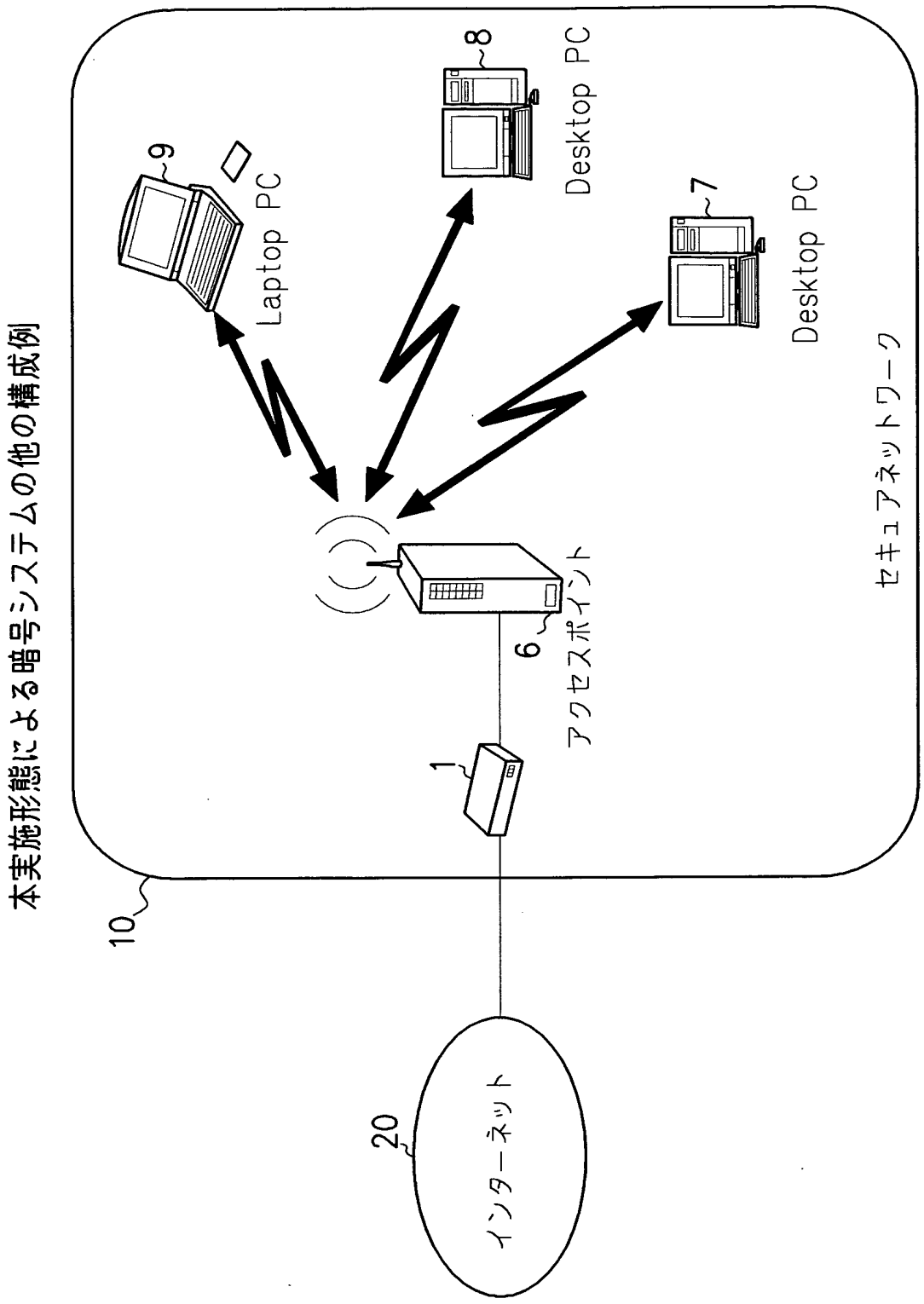

本実施形態による暗号システムの構成例
10
9
Laptop PC
8
Desktop PC
6
アクセスポイント
7
Desktop PC
HUB
5
セキュアネットワーク
1
1
1
11
11
11
2
3
4
ネットワークプリンタ
DBサーバ
ネットワークターミナル

【図２】

本実施形態による暗号システムの他の構成例

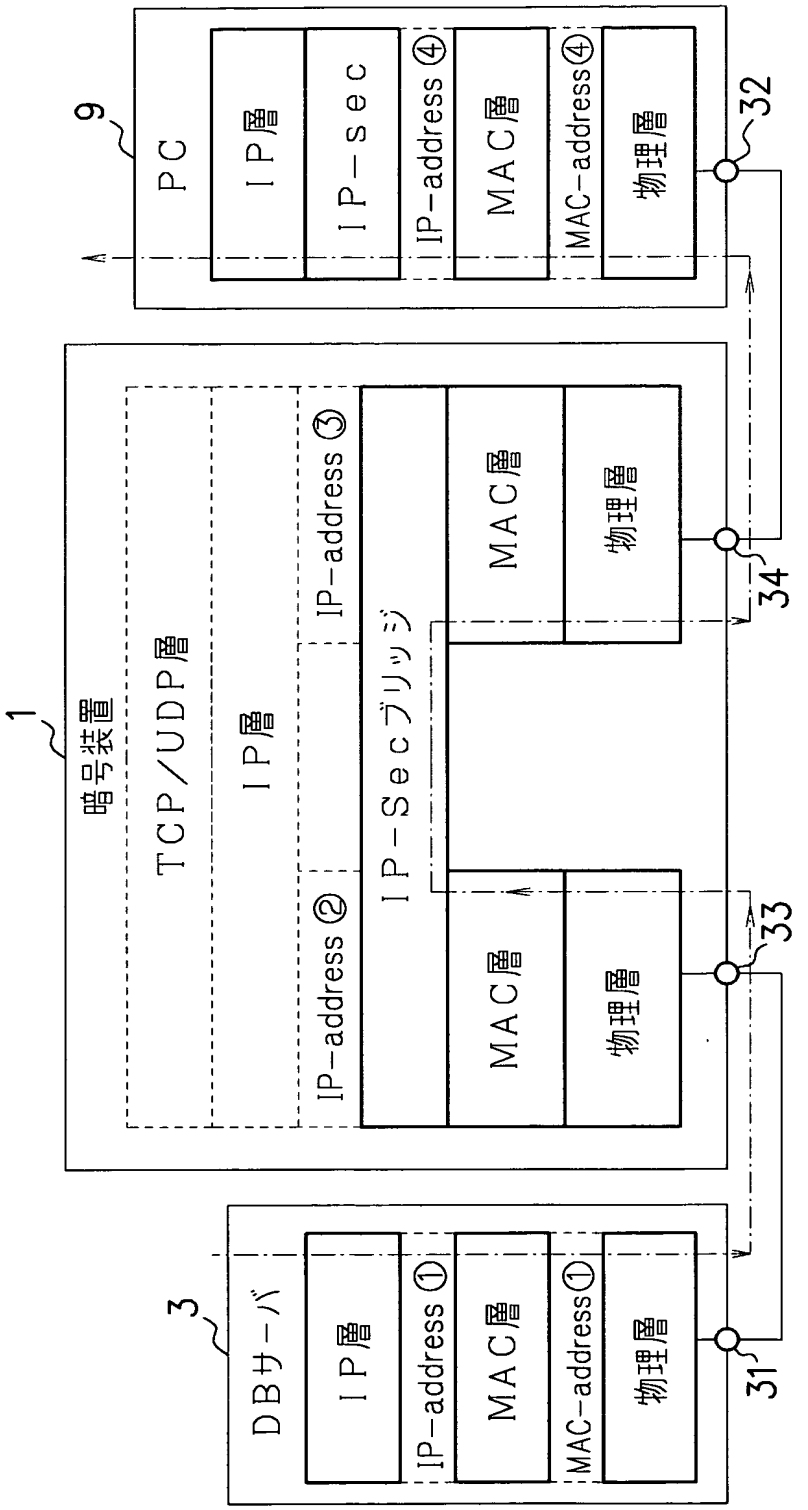


【図３】


本実施形態による暗号システムの他の構成例
10
セキュアネットワーク
1
6
アクセスポイント
7
Desktop PC
8
Desktop PC
9
Laptop PC
20
インターネット

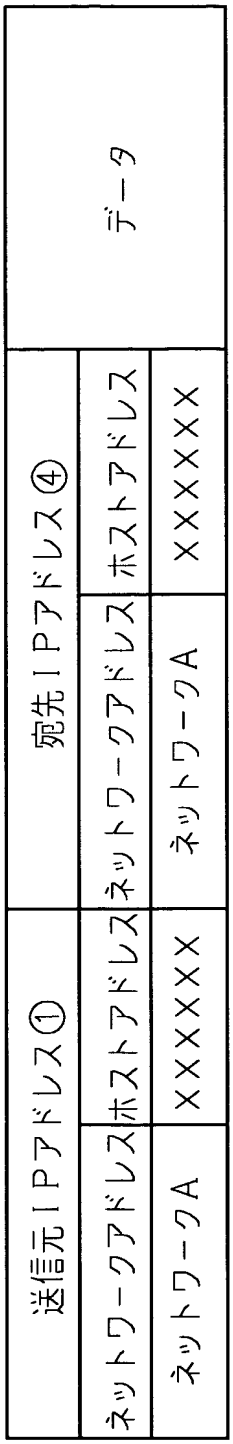
【図４】

本実施形態による暗号装置のレイヤ構造



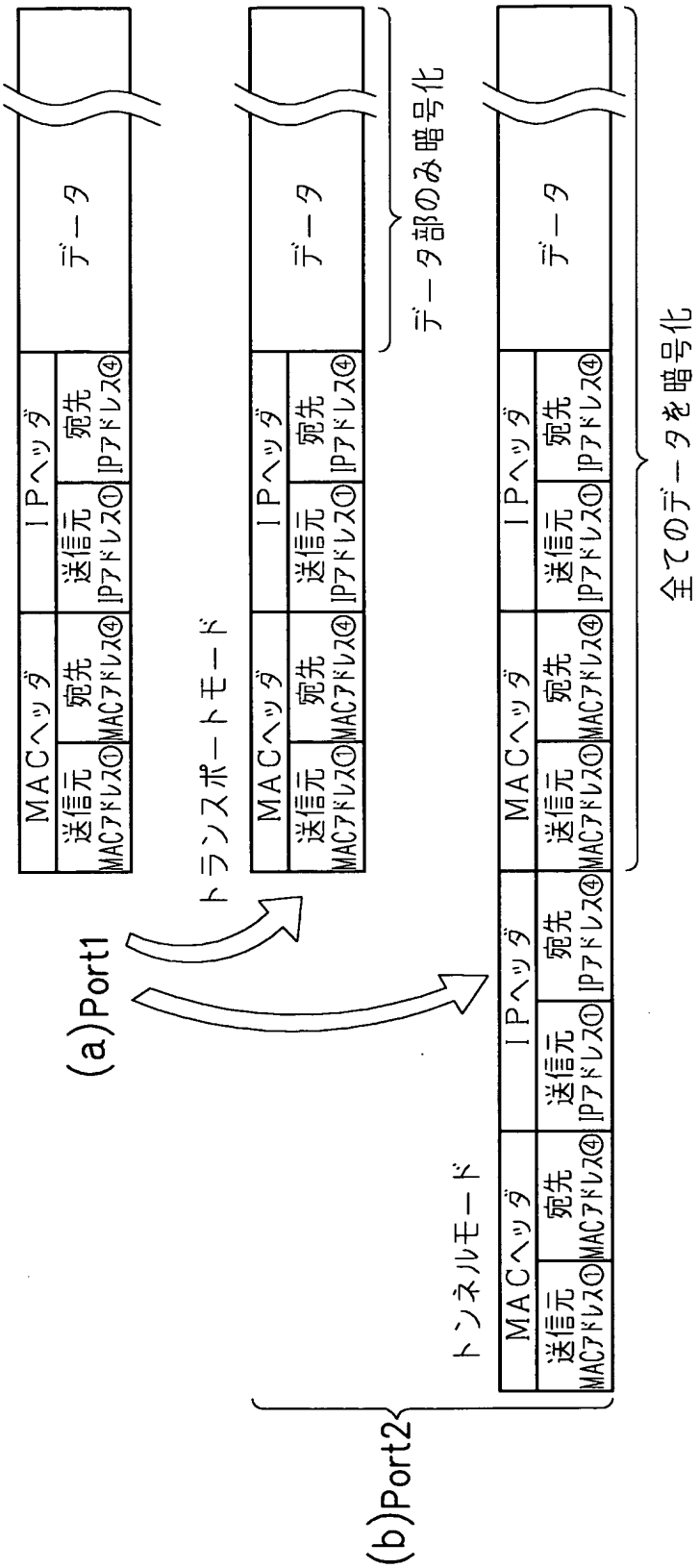
【図５】

本実施形態のパケット

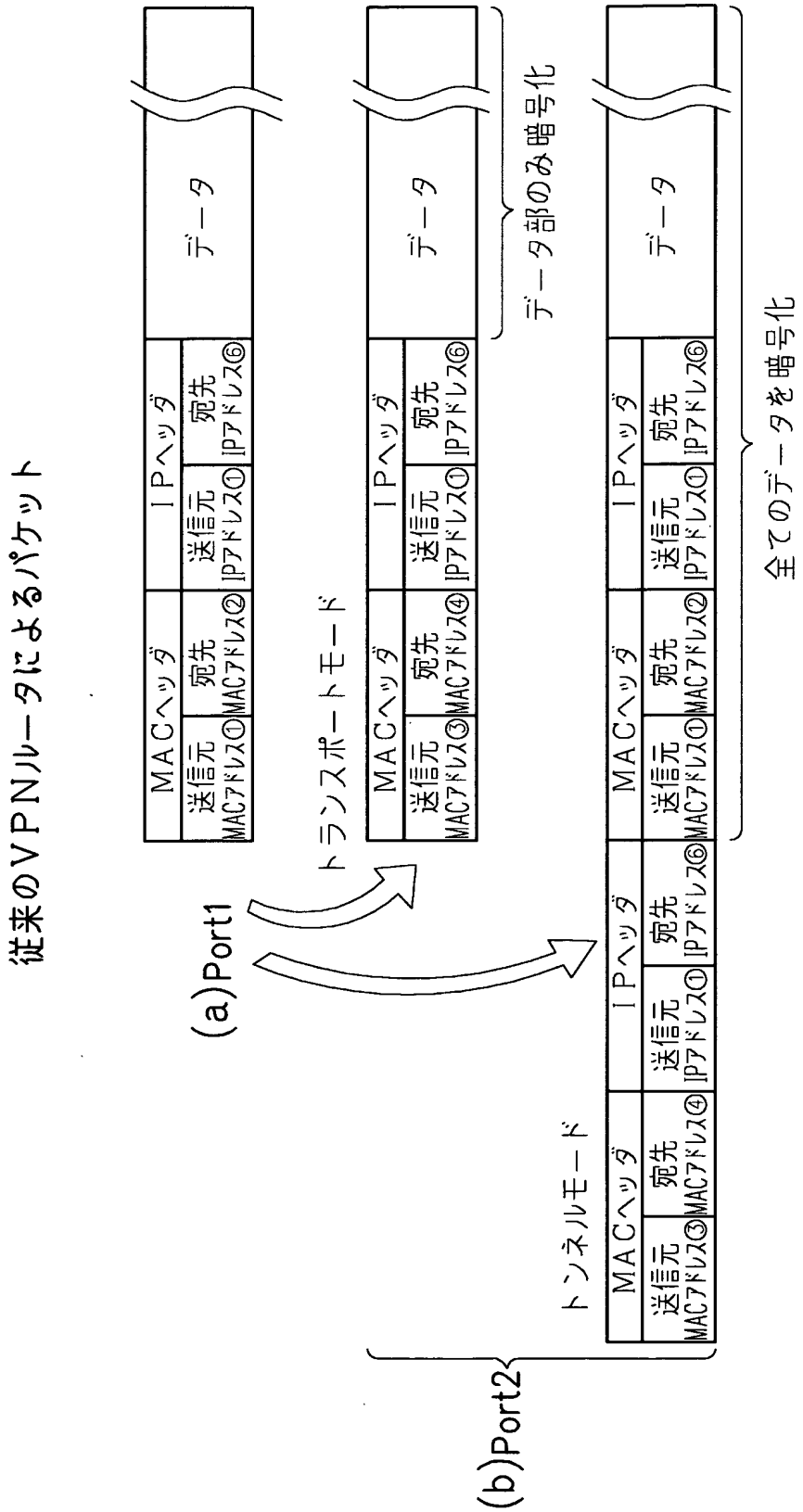


【図６】

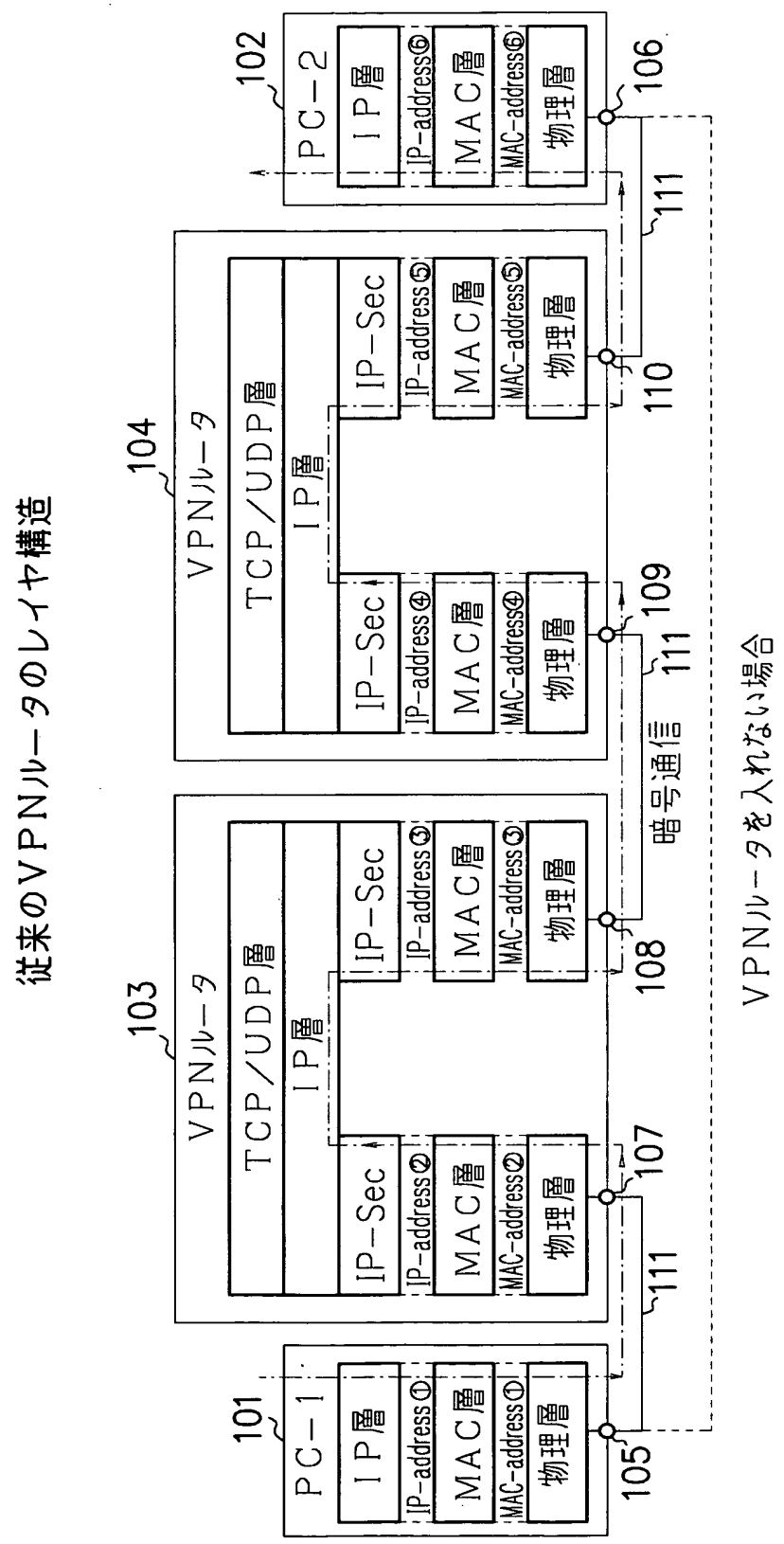
本実施形態の暗号装置によるパケット



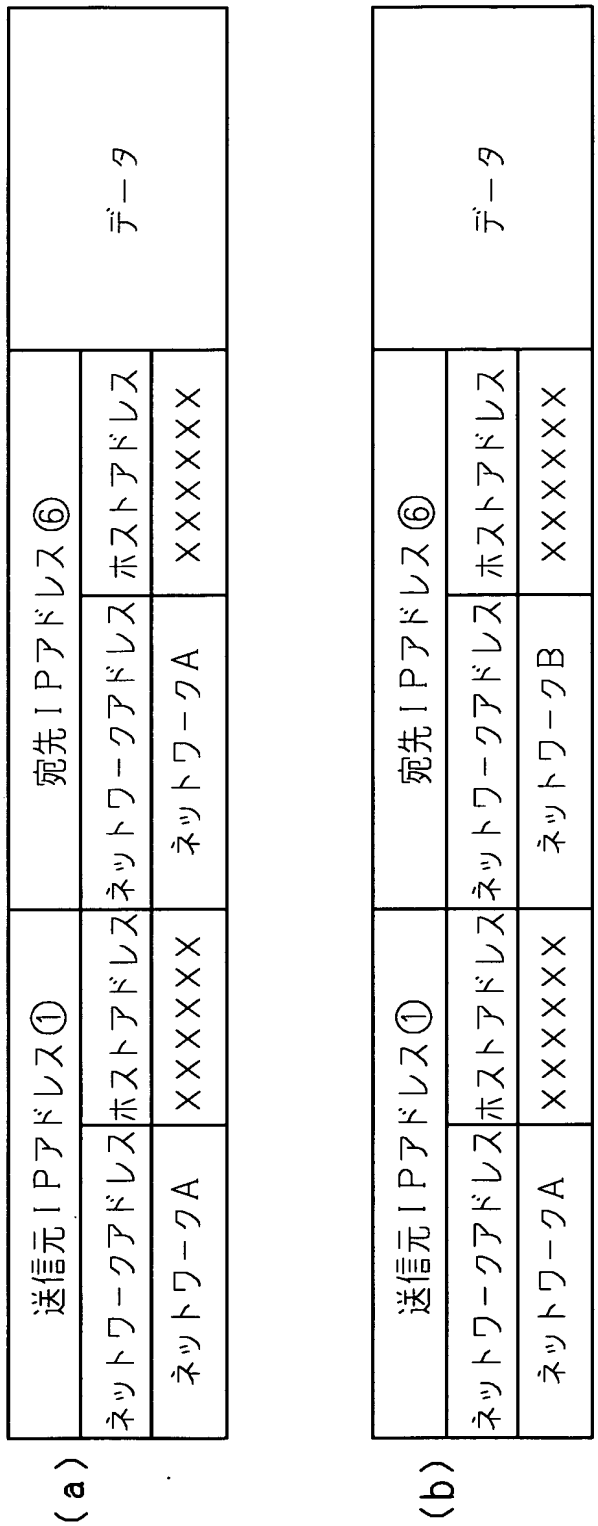
【図７】


従来のVPNルータによるパケット
(a)Port1
トランスポートモード
MACヘッダ
送信元MACアドレス①
宛先MACアドレス②
IPヘッダ
送信元IPアドレス①
宛先IPアドレス⑥
データ
MACヘッダ
送信元MACアドレス③
宛先MACアドレス④
IPヘッダ
送信元IPアドレス①
宛先IPアドレス⑥
データ
データ部のみ暗号化
(b)Port2
トンネルモード
MACヘッダ
送信元MACアドレス③
宛先MACアドレス④
IPヘッダ
送信元IPアドレス①
宛先IPアドレス⑥
MACヘッダ
送信元MACアドレス①
宛先MACアドレス②
IPヘッダ
送信元IPアドレス①
宛先IPアドレス⑥
データ
全てのデータを暗号化

【図８】


従来のＶＰＮルータのレイヤ構造
101
PC－1
IP層
IP-address①
MAC層
MAC-address①
物理層
103
VPNルータ
TCP／UDP層
IP層
IP－Sec
IP-address②
MAC層
MAC-address②
物理層
104
VPNルータ
TCP／UDP層
IP層
IP－Sec
IP-address③
MAC層
MAC-address③
物理層
102
PC－2
IP層
IP-address④
MAC層
MAC-address④
物理層
IP－Sec
IP-address⑤
MAC層
MAC-address⑤
物理層
IP層
IP-address⑥
MAC層
MAC-address⑥
物理層
105
106
107
108
109
110
111
111
111
暗号通信
ＶＰＮルータを入れない場合

【図９】


VPNルータの有無によるパケットの違い
(a)
送信元IPアドレス①
宛先IPアドレス⑥
データ
ネットワークアドレス
ホストアドレス
ネットワークアドレス
ホストアドレス
ネットワークA
XXXXXX
ネットワークA
XXXXXX
(b)
送信元IPアドレス①
宛先IPアドレス⑥
データ
ネットワークアドレス
ホストアドレス
ネットワークアドレス
ホストアドレス
ネットワークA
XXXXXX
ネットワークB
XXXXXX

【書類名】　　要約書

【要約】

【課題】　専用の暗号ソフトをインストールできない端末を有する企業内ＬＡＮの中でも暗号を利用できるようにする。

【解決手段】　暗号ソフトがインストールされたパソコン７～９との間で暗号化によるセキュリティを終端するために暗号化処理および暗号の復号化処理を行う暗号装置１を設け、例えば暗号ソフトがインストールされていない端末２～４とパソコン７～９との間に接続することにより、専用の暗号ソフトをインストールできない端末２～４を有する企業内ＬＡＮの中でも暗号を利用することができるようにして、外部からの不正侵入や攻撃によってＬＡＮ内部の機密情報が盗まれる危険性が少ないセキュアなネットワーク１０を構築することができるようにする。

【選択図】　　図１

特願２００２－１３４６８０

出　願　人　履　歴　情　報

識別番号　　［５９１２２０８５０］

１．変更年月日　　１９９６年　５月　９日
［変更理由］　　住所変更
住　所　　新潟県上越市西城町２丁目５番１３号
氏　名　　新潟精密株式会社

特願２００２－１３４６８０

出　願　人　履　歴　情　報

識別番号　［５０１３０６９７７］

１．変更年月日　２００１年　８月　２日
［変更理由］　新規登録
住　所　東京都品川区南品川２丁目２番５号
氏　名　株式会社マイクロ総合研究所